Realtime Dynamic Binary Instrumentation

Mike Du, James H. Hill

Department of Computer and Information Science

Abstract:

We present a novel technique and framework for decreasing instrumentation overhead in software systems that utilize dynamic binary instrumentation. First, we introduce a lightweight networking framework combined with an easily extensible BSON implementation as a heavy analysis routine replacement. Secondly, we bind instrumentation and analysis threads to non-overlapping cpu cores---allowing analysis threads to execute faster. Lastly, we utilize a lock-free buffering system to bridge the gap between instrumentation and analysis threads, and minimize the overhead to the instrumentation threads. Using this combination, we managed to write a dynamic binary instrumentation tool (DBI) in Pin using Pin++ that is 1100% faster than its counterpart DBI tool with no buffering, and less than 500% slower than a similar tool with no analysis routine.